BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

INTERNET-MARKs: Clear, Secure, and Portable Visual Marks for the Cyber Worlds

Hiroshi Yoshiura, Seiichi Susaki, Yasuhiko Nagai, Tsukasa Saitoh, Hisashi Toyoshima, Ryoichi Sasaki, and Satoru Tezuka

Systems Development Laboratory, Hitachi, Ltd.,
292 Yoshida-cho, Totsuka-ku, Yokohama, 244-0817 Japan
{last.name}@sdl.hitachi.co.jp

Abstract. Visual marks play critical roles in the physical world, but their use in the cyber world is limited because there they are easy to forge, tamper with and copy onto unauthorized data. This paper therefore describes a new type of visual marks that are secure because digital signatures are embedded in them and that can be used with a wide variety of cyber-world systems. It also shows the effectiveness of these marks by describing their application to WWW site authentication.

1 Introduction

Visual marks are widely used in the physical world, where they are familiar to nonprofessional people and can convey information briefly and clearly. As the cyber world becomes more and more like the physical world – filled with money, mail, and shops used by nonprofessional people – there is an increasing need for visual marks in the cyber world. The simple incorporation of visual marks, however, causes serious problems because in the cyber world these marks are easy to forge, tamper with, and copy onto unauthorized data. Visual marks suitable for use in the cyber world must be clear (i.e., easily understood) and must be secure (not easily forged, tampered with, or copied onto unauthorized data). They must also be portable, or easy to use on the wide variety of continuously evolving systems making up the cyber world. This paper describes a new type of visual marks meeting these requirements.

Sect. 2 proposes the new visual marks named INTERNET-MARKs, Sect. 3 describes an application of INTERNET-MARKs to WWW site authentication. Sect. 4 compares INTERNET-MARKs with alternative approaches, and Sect. 5 concludes the paper.

2 INTERNET MARKs

INTERNET-MARKs are made of drawings and are simply image data, such as bitmap graphics or JPEG files. They are placed on data that represent objects in the cyber world, and they carry information about the data. Actual operations of "placing I-MARKs" may be pasting the corresponding bitmap or JPEG on the data.

M. Roe et al. (Eds.): Security Protocols, LNCS 1796, pp. 195–202, 2000.

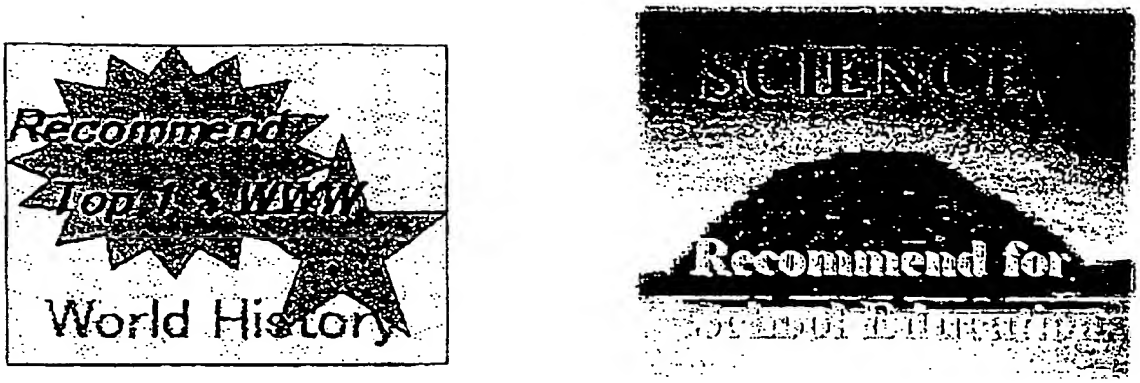

Fig. 1. Examples of FIGUREs

2.1 Basic Structure

We define some terminology.

FIGUREs drawings from which INTERNET-MARKs are made.
DATA data on which I-MARKs are placed.

Fig. 1 shows examples of FIGUREs. We also abbreviate INTERNET-MARKs and digital signatures as I-MARKs and signatures respectively. As shown in Fig. 2, an I-MARK is a simply FIGURE into which a signature is embedded by digital watermarking [1]. This signature is a signature for both the FIGURE and the DATA on which the I-MARK is pasted. Additional application-specific information may also be embedded into the FIGURE.

2.2 Security Systems

An I-MARK is issued (Fig. 2) by having the issuer sign for the DATA and the FIGURE and embedding the signature in the FIGURE. And as shown in Fig. 3, an I-MARK is verified by first cutting it out of the DATA and then extracting and verifying the signature. If the verification succeeds the system guarantees the following:

- The I-MARK is not forged and has not been tampered with.
- The I-MARK is on authorized data.
- The DATA has not been tampered with.
- The I-MARK was generated and placed on the DATA by the person indicated by the verification key (public key).

2.3 Properties

(1) Clarity
I-MARKs are easily understood because the watermarking does not degrade the clarity of the FIGUREs from which they are made.

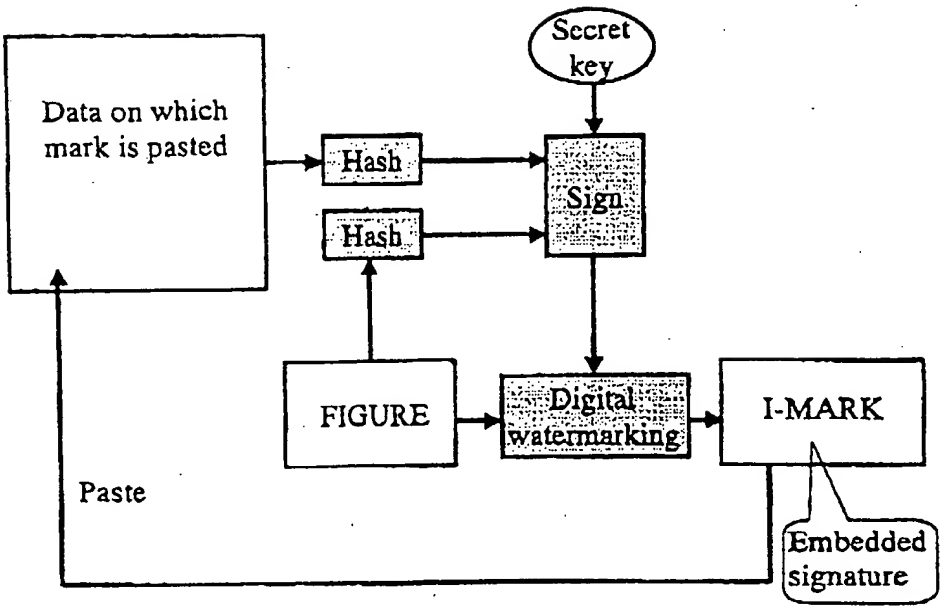

Fig. 2. INTERNET-MARK issuing system.White and black represent data and processes respectively

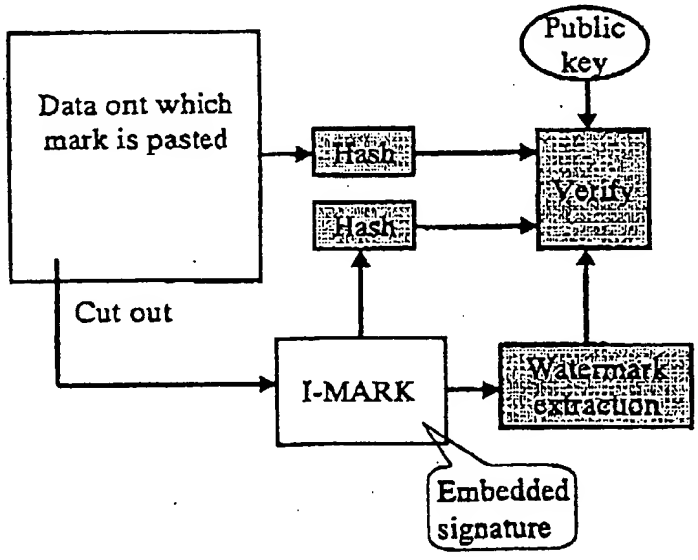

Fig. 3. INTERNET-MARK verifying system

(2) Security
It is obvious from Fig. 2 and Fig. 3 that the security of I-MARKs is equivalent to that of their underlying signatures.

(3) Portability
Equivalent clarity and security could be provided by using a simple combination of visual marks and digital signatures, but I-MARKs are more portable than the simple combination because the clarity measures (visual figures) and the security measures (digital signatures) are amalgamated in a single object.

3 An Application of INTERNET MARKs

This chapter illustrates the effectiveness of I-MARKs by describing their application to a WWW guaranteeing problem. There are three players in this application problem:

- WWW site owner (abbreviated as Owner).
- WWW site user who accesses the Owner's WWW site (User).
- Person who issues a guarantee for the Owner's WWW site (Guarantor).

When the owner asks the guarantor to issue a guarantee for owner's WWW site, the guarantor issues it and sends it to the owner, who places it on the pages of the WWW site. The guarantee may be a rating of the site, a certification of its suitability for use in schools, or any other information relevant to the site. The user accessing the site can get information about it simply by looking at the guarantee and can verify the guarantee when necessary (e.g., when sending a credit card number to the site).

We use I-MARKs for guarantees, and Fig. 4 shows that the system for issuing these guarantee I-MARKs is simply the basic I-MARK issuing system extended to include a signature for IP address of the WWW site to be guaranteed. This signature is needed to prevent WWW site disguise: the copying of both the WWW page data and its guarantee to the WWW site of an attacker who pretends to be the legal owner of its contents.

3.1 Protocols of the Application System

We first define some terminology.

SK_x	secret key of player x.
PK_x	public key of player x.
Enc(DATA,K)	result of encrypting DATA with key K.
IP-ADRESS	IP address of the WWW site to be I-MARKed.
W-DATA	DATA defining pages of the WWW site. This may be HTML source codes.
X | Y	concatenation of data X and Y.

The protocols for issuing and authenticating I-MARKs are illustrated in Fig. 5, and there are four steps in the protocol for issuing them.

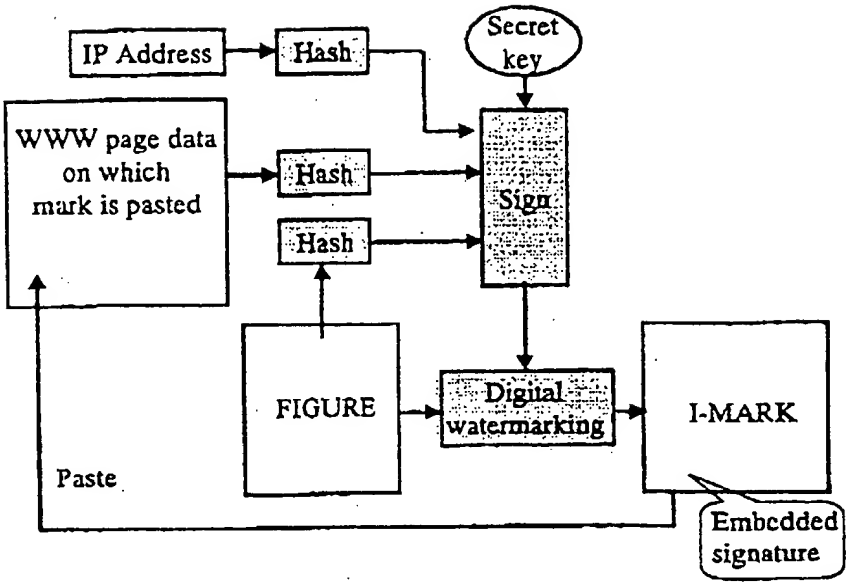

Fig. 4. System issuing an INTERNET-MARK for WWW authentication

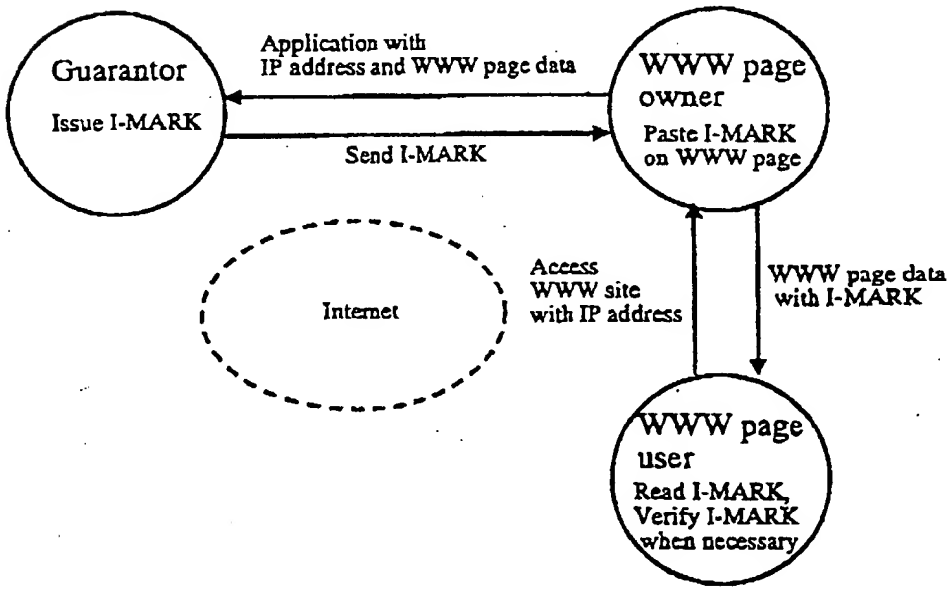

Fig. 5. Protocols for INTERNET-MARK application

Step1 The owner applies for an I-MARK by sending Enc(IP-ADRESS | W-DATA | Memo,SK_{Owner}) to the guarantor. Memo specifies the kind of I-MARK the owner wants.

Step2 The guarantor issues an I-MARK by the following substeps:

(2 - 1) Obtain the IP-ADDRESS,W-DATA,and Memo by using PK_{Owner} to decrypt the application.

(2 - 2) Select a FIGURE appropriate to the Memo and then generate a signature for the FIGURE, IP-ADRESS, and W-DATA. This signature is Enc(Hash(FIGURE) | Hash(IP-ADRESS) | Hash(W-DATA), $SK_{Guarantor}$).

(2 - 3) Generate an I-MARK by embedding the signature in the FIGURE.

Step3 The guarantor sends Enc(I-MARK,$SK_{Guarantor}$) to the owner.

Step4 The owner pastes the I-MARK on the WWW page.

The protocol for authenticating I-MARKs has 3 steps.

Step1 A user accesses the owner's WWW site by using an IP address.

Step2 The owner sends WWW data (i.e., HTML source codes) accompanied with an I-MARK to the user.

Step3 The user gets information by looking at the I-MARK and when necessary verifies the I-MARK by the following substeps:

(3 - 1) Cut the I-MARK from the WWW data, and extract the signature from the I-MARK.

(3 - 2) Verify the signature by using $PK_{Guarantor}$.In the verification, hash values are calculated for the HTML source codes and IP address of the accessed site and for the FIGURE that was used to make the I-MARK.

(3 - 3) If the verification succeeds, the protocol guarantees the followings:

- The accessed WWW site is the one for which the guarantor issued an I-MARK.
- The I-MARK is on the intended W-DATA.
- Neither the I-MARK nor the W-DATA have been tampered with.

3.2 Properties

These application protocols have been implemented in C language, and Fig. 6 shows I-MARKs made from the FIGUREs in Fig. 1. A roughly 2-K bit digital signature is embedded in each I-MARK.

(1) Clarity
As can be seen by comparing Fig. 1 and Fig. 6, the clarity of the FIGUREs is not degraded by watermarking.

(2) Security
Four types of attack are possible.

Type1 Attack I-MARKs themselves, i.e., forging and tampering with I-MARKs.

Type2 Copy I-MARKs onto unauthorized data.

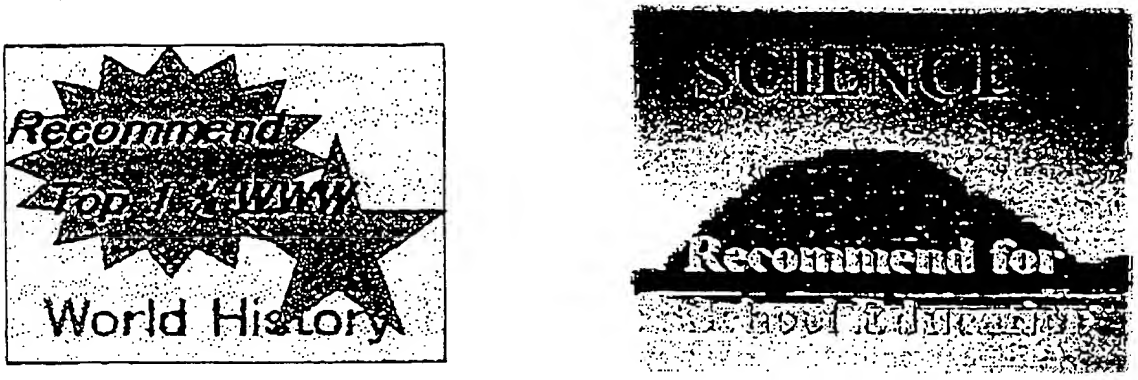

Fig. 6. INTERNET-MARKs generated from FIGUREs in Fig. 1

Type3 Copy both a WWW page data and its I-MARK to the WWW site of an attacker who pretends to be the legal owner of the WWW data.

Type4 Intervene in communication between the owner and guarantor to tamper with the owner's application for an I-MARK and with the guarantor's returning the I-MARK.

As mentioned in previous chapter, the security against first and second types of attacks is equivalent to that of their underlying signature. The security against third type is also the same as that of the signature because I-MARKs contain the signature for IP address of the correct WWW site. The security against fourth type is guaranteed by the public-key cryptosystem used in Step 1 and Step 3 of issuing I-MARKs.

(3) Portability
This issue will be discussed in next chapter by comparing I-MARKs with alternative approaches.

4 Comparison with Alternative Approaches

This chapter compares I-MARKs with the following three alternative approaches to the WWW guarantee problem.

- Simple Marks: The guarantor issues a mark that the owner attaches to the WWW page.
- Simple Signatures: The guarantor issues a signature for WWW page, and the owner attaches it to the page.
- Simple Combination of Marks and Signatures: The guarantor issues a mark and signature for both the WWW page and the mark. The owner attaches the mark and signature to the page.

It is clear from the comparison results summarize in Table 1 that simple marks are clear and portable but are of course not secure. And because a digital signature expresses nothing by itself, it tells a WWW user nothing about the

WWW page unless the user goes through the verification process. Simple signatures, although secure and reasonably portable, thus do not meet a user's needs because their meaning are not clear.

A WWW owner using a combination of marks and signatures needs to attach a mark and the corresponding signature to the WWW page in a way that there is a link between them (e.g., clicking the mark causes the signature to be verified). This attachment needs to be standardized so that WWW users can use a common program to verity signatures. Such standardization requires extensive and continuous efforts because the languages for describing WWW pages are continuously evolving as are the WWW managing systems. I-MARKs also require standardization, but this standardization should be much easier because only the way of attaching I-MARKs needs to be standardized. That is, there is no need for standardization of the ways of attaching signatures and of linking marks and signatures.

Table 1. Comparison with Alternative Approaches

Methods	Security	Understandability	Portability
Simple marks	NG	Good	Good
Simple signatures	Good	NG	Not so bad
Simple combination of marks and signatures	Good	Good	NG
INTERNET-MARKs	Good	Good	Not so bad

5 Conclusion

This paper proposed a new type of visual marks suitable for use in the cyber world. The paper has shown that INTERNET-MARKs are as easily understood as conventional visual marks, are as secure as digital signatures, and are more portability than a simple combination of visual marks and digital signatures.

Acknowledgements

This research is supported by the Ministry of Posts and Telecommunications of Japan and the Telecommunications Advancement Organization of Japan.

References

1. M Swanson, M Kobayashi, and A Tewfik,: Multimedia Data-Embedding and Watermarking Technologies. Proceedings of the IEEE, Vol. 86, No.6, 1998, pp.1064–1087.

Lecture Notes in Computer Science 1796

Bruce Christianson Bruno Crispo
James A. Malcolm Michael Roe (Eds.)

Security Protocols

7th International Workshop
Cambridge, UK, April 1999
Proceedings

Springer